Configuring NAT

This section provides information to configure NAT using the command line interface.

Topics in this section include:

ISA Redundancy

The 7750 SR supports ISA redundancy to provide reliable NAT even when an MDA fails. The active-mda-limit allows an operator to specify how many MDAs will be active in a given NAT group. Any number of MDAs configured above the active-mda-limit will be spare MDAs; they take over the NAT function if one of the current active MDAs fail.

A sample configuration is as follows:

```
Configure
    isa
        nat-group 1 create
            active-mda-limit 1
            mda 1/2
            mda 2/2
            no shutdown
        exit
    exit
exit
```

Show commands are available to display the actual state of a nat-group and its corresponding MDAs:

```
show isa nat-group 1
===============================================================================
ISA NAT Group 1
===============================================================================
Admin state       : inService           Operational state : inService
Active MDA limit  : 1                   Reserved sessions : 0
High Watermark (%): (Not Specified)     Low Watermark (%) : (Not Specified)
Last Mgmt Change  : 01/11/2010 15:05:36
===============================================================================
===============================================================================
ISA NAT Group 1 members
===============================================================================
Group Member     State          Mda  Addresses  Blocks     Se-% Hi Se-Prio
-------------------------------------------------------------------------------
1     1          active         1/2  0          0          0    N  0
-------------------------------------------------------------------------------
No. of members: 1
===============================================================================
```

A maximum of four nat-groups can be configured. This gives the operator the ability to differentiate between different traffic types. Normal traffic could be routed to nat-group one, where a limited number of MDA without spare MDAs are available, while high priority traffic could make use of nat-group two, where several active MDAs and a spare MDA are configured. A maximum of six MDAs per nat-group can be configured.

A nat-group cannot become active (no shutdown) if the number of configured MDAs is lower that the active-mda-limit.

A given MDA can be configured in several nat-groups but it can only be active in a single nat-group at any moment in time. Spare MDAs can be shared in several nat-groups, but a spare can only become active in one nat-group at a time. Changing the active-mda-limit, adding or removing MDAs can only be done when the nat-group is shutdown.

Nat-groups that share spare MDAs must be configured with the same list of MDAs. It is possible to remove/add spare MDAs to a nat-group while the nat-group is admin enabled.

```
Configure
    isa
        nat-group 1 create
            active-mda-limit 1
            mda 1/2
            mda 2/2
            mda 3/1
            no shutdown
        exit
        nat-group 2 create
            active-mda-limit 1
            mda 1/2
            mda 2/2
            mda 3/1
            no shutdown
        exit
    exit
exit
```

Through show commands, it is possible to display an overview of all the nat-groups and MDAs.

```
show isa nat-group
===============================================================================
ISA NAT Group Summary
===============================================================================
Mda  Group 1            Group 2
-------------------------------------------------------------------------------
1/1  active             busy
2/2  busy               active
3/1  standby            standby
===============================================================================
```

If an MDA fails, the spare (if available) will take over. All active sessions will be lost, but new incoming sessions will make use of the spare MDA.

In case of an MDA failure in a nat-group without any spare MDA, all traffic towards that MDA will be black-holed.

For L2-aware NAT, the operator has the possibility to clear all the subscribers on the affected MDA (clear nat isa), terminating all the subscriber leases. New incoming subscribers will make use of the MDAs that are still available in the nat-group.

NAT Layer 2-Aware Configurations

The following sections provide NAT Layer 2-Aware configurations.

```
#--------------------------------------------------
echo "Card Configuration"
#--------------------------------------------------
    card 1
        card-type iom3-xp
        mda 1
            mda-type m60-10/100eth-tx
        exit
        mda 2
            mda-type isa-bb
        exit
    exit
    card 2
        card-type iom3-xp
        mda 1
            mda-type m60-10/100eth-tx
        exit
        mda 2
            mda-type isa-bb
        exit
    exit

#--------------------------------------------------
echo "ISA Configuration"
#--------------------------------------------------
    isa
        nat-group 1 create
            description "1 active + 1 spare"
            active-mda-limit 1
            mda 1/2
            mda 2/2
            no shutdown
        exit
    exit
#--------------------------------------------------
echo "Router (Network Side) Configuration"
#--------------------------------------------------
    router
        ...
#--------------------------------------------------
echo "NAT (Network Side) Configuration"
#--------------------------------------------------
        nat
            outside
                pool "pool1" nat-group 1 type l2-aware create
                    address-range 81.81.0.0 81.81.0.200 create
                    exit
                    no shutdown
                exit
            exit
        exit
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        customer 1 create
```

```
            description "Default customer"
        exit
        ...
        vprn 100 customer 1 create
            ...
            nat
                outside
                    pool "pool2" nat-group 1 type l2-aware create
                        address-range 82.0.0.0 82.0.0.200 create
                        exit
                        no shutdown
                    exit
                exit
            exit
        exit

        vprn 101 customer 1 create
            ...
            nat
                inside
                    l2-aware
                        # Hosts in this service with IP addresses in these ranges
                        # will be subject to l2-aware NAT.
                        address 10.0.0.1/29
                        address 10.1.0.1/29
                    exit
                exit
            exit
        exit
        ...
        nat
            nat-policy "l2-aware-nat-policy1" create
                pool "pool1" router Base
            exit
            nat-policy "l2-aware-nat-policy2" create
                pool "pool2" router 100
            exit
        exit
        ...
    exit
#--------------------------------------------------
echo "Subscriber-mgmt Configuration"
#--------------------------------------------------
    subscriber-mgmt
        # Subscribers using these sub-profiles will be subject to l2-aware NAT.
        # The configured nat-policies will determine which IP pool will be used.
        sub-profile "l2-aware-profile1" create
            nat-policy "l2-aware-nat-policy1"
        exit
        sub-profile "l2-aware-profile2" create
            nat-policy "l2-aware-nat-policy2"
        exit
        ...
    exit
```

Large Scale NAT Configuration

The following sections provide Large Scale NAT configuration examples.

```
configure
#--------------------------------------------------
echo "Card Configuration"
#--------------------------------------------------
    card 3
        card-type iom3-xp
        mda 1
            mda-type isa-bb
        exit
        mda 2
            mda-type isa-bb
        exit
    exit
#--------------------------------------------------
echo "ISA Configuration"
#--------------------------------------------------
    isa
        nat-group 1 create
            active-mda-limit 2
            mda 3/1
            mda 3/2
            no shutdown
        exit
    exit
#--------------------------------------------------
echo "Filter Configuration"
#--------------------------------------------------
    filter
        ip-filter 123 create
            entry 10 create
                match
                    src-ip 13.0.0.1/8
                exit
                action nat
            exit
        exit
    exit
#--------------------------------------------------
echo "NAT (Declarations) Configuration"
#--------------------------------------------------
    service
        nat
            nat-policy "ls-outPolicy" create
            exit
        exit
    exit
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        customer 1 create
            description "Default customer"
        exit
        vprn 500 customer 1 create
            interface "ip-113.0.0.1" create
            exit
```

```
            nat
                outside
                    pool "nat1-pool" nat-group 1 type large-scale create
                        port-reservation ports 200
                        address-range 81.81.0.0 81.81.6.0 create
                        exit
                        no shutdown
                    exit
                exit
            exit
        exit
        vprn 550 customer 1 create
            interface "ip-13.0.0.1" create
            exit
        exit
        nat
            nat-policy "ls-outPolicy" create
                pool "nat1-pool" router 500
                timeouts
                    udp hrs 5
                    udp-initial min 4
                exit
            exit
        exit
        vprn 500 customer 1 create
            router-id 10.21.1.2
            route-distinguisher 500:10
            vrf-target export target:500:1 import target:500:1
            interface "ip-113.0.0.1" create
                address 113.0.0.1/24
                static-arp 113.0.0.5 14:99:01:01:00:01
                sap 1/1/1:200 create
                exit
            exit
            no shutdown
        exit
        vprn 550 customer 1 create
            router-id 10.21.1.2
            route-distinguisher 550:10
            vrf-target export target:550:1 import target:550:1
            interface "ip-13.0.0.1" create
                address 13.0.0.1/8
                sap 1/2/1:900 create
                    ingress
                        filter ip 123
                    exit
                exit
            exit
            nat
                inside
                    nat-policy "ls-outPolicy"
                exit
            exit
            no shutdown
        exit
    exit
exit all
```

NAT Configuration Examples

The following output displays example configurations.

VPRN service example:

```
configure service vprn 100 nat
                inside
                    nat-policy "priv-nat-policy"
                    destination-prefix 0.0.0.0/0
                    dual-stack-lite
                        subscriber-prefix-length 128
                        address 2001:470:1F00:FFFF::190
                            tunnel-mtu 1500
                        exit
                        no shutdown
                    exit
                    redundancy
                        no peer
                        no steering-route
                    exit
                    subscriber-identification
                        shutdown
                        no attribute
                        no description
                        no radius-proxy-server
                    exit
                    l2-aware
                    exit
                exit
                outside
                    no mtu
                exit
```

Router NAT example:

```
configure router nat
            outside
                no mtu
                pool "privpool" nat-group 3 type large-scale create
                    no description
                    port-reservation blocks 128
                    port-forwarding-range 1023
                    redundancy
                        no export
                        no monitor
                    exit
                    subscriber-limit 65535
                    no watermarks
                    mode auto
                    address-range 13.0.0.5 13.0.0.6 create
                        no description
                        no drain
                    exit
                    no shutdown
                exit
                pool "pubpool" nat-group 1 type large-scale create
                    no description
```

```
                port-reservation blocks 1
                port-forwarding-range 1023
                redundancy
                    no export
                    no monitor
                exit
                subscriber-limit 65535
                no watermarks
                mode auto
                address-range 138.203.8.241 138.203.8.247 create
                    no description
                    no drain
                exit
                no shutdown
            exit
        exit
```

Service NAT example:

```
configure service nat
        nat-policy "priv-nat-policy" create
            alg
                ftp
                rtsp
                sip
            exit
            block-limit 4
            no destination-nat
            no description
            filtering endpoint-independent
            pool "privpool" router Base
            no ipfix-export-policy
            port-limits
                forwarding 64
                no reserved
                no watermarks
            exit
            priority-sessions
            exit
            session-limits
                max 65535
                no reserved
                no watermarks
            exit
            timeouts
                icmp-query min 1
                sip min 2
                no subscriber-retention
                tcp-established hrs 2 min 4
                tcp-syn sec 15
                no tcp-time-wait
                tcp-transitory min 4
                udp min 5
                udp-initial sec 15
                udp-dns sec 15
            exit
            no tcp-mss-adjust
            no udp-inbound-refresh
        exit
        nat-policy "pub-nat-policy" create
```

```
        alg
            ftp
            no rtsp
            no sip
        exit
        block-limit 1
        no destination-nat
        no description
        filtering endpoint-independent
        pool "pubpool" router Base
        no ipfix-export-policy
        port-limits
            no forwarding
            no reserved
            no watermarks
        exit
        priority-sessions
        exit
        session-limits
            max 65535
            no reserved
            no watermarks
        exit
        timeouts
            icmp-query min 1
            sip min 2
            no subscriber-retention
            tcp-established hrs 2 min 4
            tcp-syn sec 15
            no tcp-time-wait
            tcp-transitory min 4
            udp min 5
            udp-initial sec 15
            udp-dns sec 15
        exit
        no tcp-mss-adjust
        no udp-inbound-refresh
    exit
```